REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

The specification has been amended to correct the informalities noted in the office action and other informalities noted during preparation of this response.

Claim 2 was rejected under 35 U.S.C. Section 112, second paragraph, as allegedly being indefinite because of the reference to "information b". "Information" has been deleted to clarify that "b" refers to the size of the previously recited private key "p". Claim 11 has been similarly amended.

Claims 1-13 were rejected under 35 U.S.C. Section 112, first paragraph, as allegedly being based on a non-enabling disclosure. Applicants traverse this rejection for at least the following reasons.

According to the Fermat's theorem, if p is a prime number and g is not divisible by p, then

$g^{p-1} \equiv 1 (\text{mod } p)$.

When such a congruence expression does not hold for g that is a positive integer smaller than p-1, g is referred to as a primitive element modulo p or a primitive generator modulo p.

Generally, if $g^e = 1 (\text{mod } p)$ where e is a positive integer smaller than p, e is a divisor of p-1. If $g^e \equiv 1 (\text{mod } p)$ where e is a least positive integer, e is referred to as a period. If the period e satisfies a maximal period e=p-1, g is a primitive element. Therefore, a total number of primitive elements modulo p is $\phi(p-1)$. For example, if p=5, there exist two primitive elements, which are 2 and 8.

A general form of an expansion of Fermat's theorem is called Euler's theorem. Euler's theorem is as follows:

If there are two positive integers g, n where g is not divisible by n (g is smaller than n), then

$$g^{\phi(n)} \equiv 1 \pmod{n}$$

wherein $\phi(n)$ is an Euler function.

In a special case in which n is a product of large prime numbers p, q (n=pq), Euler's theorem is used for RSA public-key cryptography and $\phi(n) = (p-1)(q-1)$. Further, if a least common multiple of p-1 and q-1 is $L = \mathrm{lcm}\{p-1, q-1\}$, the following congruence expression equivalent to Euler's theorem holds:

$$g^{L} = 1 \pmod{n}$$

Here, the above expression does not hold for all positive integers e smaller than L (e<L). If the above expression holds for e=L, g is referred to as a maximal generator. A maximal generator modulo a composite number in Euler's theorem has a concept similar to a primitive element (primitive generator) modulo a prime number in Fermat's theorem.

$\phi(n) = (p-1)(q-1)$ is divisible by L. The power of the congruence expression in Euler's theorem means that an identical power appears repeatedly $\phi(n)/L$ times, and every time the power becomes a multiple of L, $= 1 \pmod{n}$ holds $\phi(n)/L$ times on the right side.

As to the "maximal generator g" in equations (1) and (2) of claim 1, for example, $g^{c} = 1 \pmod{n}$ does not hold for all positive integers e smaller than L (e<L). However, the "maximal generator g" becomes a positive integer such that $g^{e} = 1 \pmod{n}$ holds for e=L (L represents a least common multiple of p-1 and q-1).

The subject application is based on the RSA public key cryptography. In RSA public key cryptography, "maximal generator" is a known concept. Thus, a person skilled in the art with knowledge of the RSA public-key cryptography would understand the use of this term in the claims of the present application and withdrawal of the section 112, first paragraph rejection is respectfully requested.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,
NIXON & VANDERHYE P.C.

By: 

Michael J. Shea
Reg. No. 34,725

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
MJS:mjs